I didn't see that! An examination of Internet browser cache behaviour following web-site visits.

Graeme Horsman
Faculty of Computer Science
The David Goldman
Informatics Centre
St Peter's Way
Sunderland
SR6 0DD

Present address: -
Teesside University
School of Science, Engineering & Design
Campus Heart
Southfield Rd
Middlesbrough
TS1 3BX
United Kingdom,

Email: graeme.horsman@tees.ac.uk

Abstract
By default, all major web browsing applications cache visited website content to the local disk to improve browser efficiency and enhance user experience. As a result of this action, the cache provides a window of opportunity for the digital forensic practitioner to establish the nature of the content which was hosted on the websites which had been visited. Cache content is often evidential during cases surrounding Indecent Images of Children (IIoC) where it is often assumed that cached IIoC is a record of the content viewed by a defendant via their browser. However, this may not always be the case. This article investigates web browser cache behaviour in an attempt to identify whether it is possible to definitively establish what quantity of cached content was viewable by a user following a visit to a website. Both the Mozilla Firefox and Google Chrome browser caches are analysed following visits to 10 test websites in order to quantify cache behaviour. Results indicate that the volume of locally cached content differs between both web browsers and websites visited, with instances of images cached which would not have been viewable by the user upon landing on a website. Further, the number of cached images appears to be effected by how much of a website a user scrolls through.

Keywords: Digital Forensics; Cache; Internet; Web Browser; Cache Forensics; Images Depicting Child Sexual Abuse.

1 Introduction

The cache functionality of an Internet browser application is a well documented and discussed concept in the field of digital forensics (see The Chromium Projects, n.d.; Habben, 2015; Ritchie, 2012). Its job is to enhance a user's web-browsing experience by downloading and storing a local version of website artefacts to provide increased efficiency in the re-rendering of a website on future visits (Howard, 2004). The cache can offer an insight into the browsing

habits of a user, where although Internet history records may document the locations a user has visited online, the cache can reveal the content hosted on these webpages. Cached content can provide a vital source of evidence in many investigative scenarios and most notably, in investigations surrounding the possession, distribution and creation of Indecent Images of Children (IIoC) (see for example *United States v. Tucker*, 305 F.3d 1193 (10th Cir. 2002)).

Whilst at first glance, analysis of the cache may seem straightforward (in terms of understanding the structure of its stored data), questions regarding its functionality are raised, particularly in relation to the volume of data which is cached and when caching occurs. To provide context to cache related investigatory issues, a discussion of regulatory concerns surrounding IIoC and the web browser cache is offered. In cases where IIoC are found in a defendant's browser cache, cases often revolve around a defendant's knowledge of the cache in order to attribute some form of culpability over this content (Marin, 2008). In English law, liability for possession may ensue if a user knows of the cache (i.e. knows of its existence on their digital device), subject to legal tests of possession (see Atkins v DPP; Goodland v DPP [2000] 2 Cr. App. R. 248) and statutory defences (see Criminal Justice Act 1988 (CJA88), Section 160(2)). Of particular interest (if knowledge of the cache is established) is the CJA88 Section 160(2)(b), where a defendant may rely on a statutory defence if they can prove that they "had not himself seen the photograph [or pseudo-photograph] and did not know, nor had any cause to suspect, it to be indecent". In this situation, the requirement to have 'not seen a photograph' provides an area for exploration given that the cache is an automatic function, storing the content of visited websites. This defence requires establishing what a user has viewed on their screen, a task that during a *post mortem* investigation can only be established through analysis of cached data. Yet there is currently limited research analysing the functionality of web browser caches in terms of how much of a visited website is cached, and crucially in this context, whether it is possible to establish which (or if) content is cached without a user ever physically seeing it on their screen. Establishing with accuracy which cached files were viewable on screen and which were not, may support the application of the defence under CJA88 Section 160(2)(b) (and equivalent international law regarding a defence involving sight) with a greater degree of reliability.

This article provides a discussion of the functionality of the Mozilla Firefox and Google Chrome Internet browsing applications, not from an information-parsing standpoint, but from a behavioural context. The digital footprint left behind in the cache of each browser is examined and correlated against standard user browsing behaviour (both on landing and following a page scroll) in order to establish whether through cached-content, it is possible to identify which parts of a website were visually present on-screen and arguably viewed by a user.

2 The Cache

Although the structure of the cache differs between browsing applications (see discussions by Altheide and Carvey, 2011), its overarching functionality remains the same; to improve browsing performance. Cache setups are configurable by the user or in some cases can be turned off (with performance detriments), however, by default, all mainstream browsing applications dedicate a region of local storage media for the caching of website artefacts which can include text, media, application and site structural content. As cache content is utilised in the rebuilding of websites by a browser upon a re-visit by the user, cache content can also support the offline rebuilding of webpage content during forensic investigations (see tools such as NetAnalysis

(Digital Detective, 2017) and IEF (Magnet Forensics, 2017)). However, Casey (2009) expresses the need for caution when undertaking such processes due to the potential for unreliable results due to the high turnover of files in the cache where multiple artefacts maybe similarly named and lead to inaccurately rebuilt pages. Even without cached page rebuilding, it may be possible to correlate the creation time and date of individual cached artefacts against Internet history records to identify websites which were visited and of evidential value. This is often a process involved in IIoC investigations where the Internet now often provides a main source of this material (Horsman, 2016).

2.1 IIoC and the cache

IIoC found in the Internet browser has been the subject to legal debate where arguments are offered both in terms of an offence of possession and that of making (Marin, 2008). The difficulty lies with the fact that the function of a web-browser cache is automated by design, which subsequently allows imagery hosted on browsed websites to be collected and stored.

The function of the cache is legitimate, but assigning culpability for its content poses issues. To determine whether a defendant is guilty of an offence of possession in regards to IIoC stored in their browser cache, a question of what constitutes a person having 'possession' of the cache's content is crucial. In English law, a possession offence is offered under Section 160 CJA88 where possession involves both a physical and mental element (CPS, 2017). To be in possession of cached images a defendant must have custody and control of the images (be able to retrieve/access them) and knowledge of the images following *Atkins v DPP; Goodland v DPP [2000] 2 Cr. App. R. 248*, where a defendant's knowledge of the existence of the browser cache must be established. To try and simplify, a defendant cannot be in possession of an IIoC if they do not know about its presence on their system, and following *R v Porter [2006] EWCA Crim 560*, to have custody and control over an image, a defendant must be able to access that image. Where both knowledge and, 'custody and control' are established, a defendant is deemed to have possession of an image. In this instance, a defendant may seek to rely on one of the three statutory defences under the CJA88 Section 160(2) if they can prove (on the balance of probabilities) that they had a legitimate reason for possessing an image, that they had not seen the image or suspected it to be indecent, or finally, that the image was sent without any prior request and it was not kept an unreasonable amount of time (Wall, 2017). To circumvent the difficulties associated with establishing possession, particularly involving the cache, where there is evidence of a deliberate intentional act (see *R v Bowden* [2000] 1 Cr. App. R. 438), such as searching for IIoC online, a charge of 'making' may be attributed.

Under normal browsing circumstances consideration as to what a user of a web browser has actually physically seen on their screen is of little evidential value. Yet in cases of IIoC, the cache is assumed to be a record of what a defendant has viewed leading to potential liability, as noted above. Cached IIoC provide an insight into the severity of the offence committed (see CPS (2017) for categorisation and sentencing guidance), but limited consideration is given as to whether these images have actually been physically seen by a defendant. Arguably this stems from a lack of complete understanding, not at a technical, but functional level of the web browser cache. Although the technical cache structure is relatively well documented (see The Chromium Projects, n.d.; Habben, 2015; Ritchie, 2012), often by those involved in forensic analysis, there is limited research available demonstrating the impact on the cache

caused by standard user browsing actions. To place this in context, focus is drawn to the following quote by McBath (2012, p.389).

> "the first time a user visits a website two simultaneous processes occur: (1) the computer opens the website and shows it on the screen, and (2) the computer creates a copy of all the data on that website and stores it in the cache. Thus, an image will not be stored in the cache unless the website from which it came was, at one time, on the computer screen….Images found in the cache are simply evidence of the prior possession that the defendant had when the images were on his screen" (McBath, 2012, p.389).

This statement raises the following three generalisations regarding the cache which are arguably in need of further investigation.

1. *"The computer creates a copy of all the data on that website and stores it in the cache".*
2. *"An image will not be stored in the cache unless the website from which it came, was at one time, on the computer screen".*
3. *"Images found in the cache are simply evidence of the prior possession that the defendant had when the images were on their screen" (McBath, 2012, p.389).*

IIoC are a product used for sexual stimulation, which is arguably achieved when the imagery is physically viewed, an act often condemned (see dissenting comments in *United States v. Goff*, 501 F.3d 250, 258 (3d Cir. 2007) and McBath (2012)). Yet it may not be accurate to assume that cache content has always been visible to the user on their screen. Website structures vary greatly in shape and size and it remains a distinct possibility that users can visit a website and not physically witness all content hosted upon it without a thorough inspection. In addition, it is necessary to differentiate between a user who mistakenly visits a site and one who examines all content visually, where section 3 provides an analysis of the behaviour of the cache.

3 Cache behaviour

This article investigates the functionality of the Google Chrome and Mozilla Firefox web browser cache in an attempt to establish whether a user's viewing behaviour in terms of on-screen browser position and their scrolling actions (movement of the page on-screen), can be correlated to cached content. When the user visits a website, testing will explore the three statements extracted from McBath's (2012) noted above in section 2.2 and the following research question:

'Can we tell how much of a website has been actually viewed by a user?'

When taking into account the complexity in shape and size of modern website design, it is possible to visit a website but not visually witness all of its hosted content before moving on to another. The issue remains that in this situation, unseen components of the website may be cached and if these elements are IIoC, potential liability may occur and a defendant may be required to prove they had not seen the IIoC. This would require conclusively establishing how a cache functions when a particular suspect website was visited, and, correlating the volume of cache imagery to that found within a defendant's cache against a set of test actions.

In most investigations, the challenge lies with accurately establishing an understanding of suspect actions within their digital device. Often this must be done with limited knowledge of what a suspect has undertaken, and only the *post-mortem* remnants of their actions. Any accompanying explanation provided from a defendant may not be reliable, placing emphasis on the ability to interpret leftover remnants of data. In the case of cache analysis, a practitioner maintains elements of the cache from a particular site, with the challenge lying with determining which elements were seen. This issue can be summarised where a practitioner is presented with the statement of *'I did not see the content stored on the website'*. In some cases, evidence of visiting a particular website may be enough to prosecute. However, establishing how much of the website they viewed can differentiate between someone who truly mistakenly visits and someone who has taken additional time to view content, potentially providing evidence of a defendant's mind set and intent.

Section 3.1 provides a discussion of web browser positions and an example cache examination documenting resident cache content following a visit to www.bbc.co.uk/news. Section 3.2 offers the results of 10 subsequent cache examinations following test website visits.

3.1 Browser position

A browser's position denotes what a user can see on their screen and provides a starting point for cache discussions. Given the diversity of website design, many domains maintain bespoke structures. Soasta in 2015 reported the average webpage to be around 2MB in size, (increasing to around 3MB in 2017 (httparchive, 2017)) maintaining complex structural elements, which ultimately will impact the content which is cached locally. However, browser resolution dictates what a user sees on-screen upon first visit to a site (coined 'on-landing'). This section of the website is often referred to as 'above the fold', a term derived from publishing industries and typically allows the top 600-1000 pixels (15.9*26.5cm) of a website to be viewed without scrolling (Miller, 2016). To provide an example, Figure 1 provides a visual (wireframe) breakdown of the images which are cached on-landing, above the fold from a visit to the 'www.bbc.co.uk/news' website. The dimensions of the bbc.co.uk/news webpage were 141cm*31cm, converted from pixel measurements. Wireframe 1 highlights cached images by the Mozilla Firefox on-landing. Wireframe 2 documents cached images by the Chrome browser on-landing. The red line indicates the bottom of the screen, where content above was viewable by the user on landing. Red blocks indicate a hosted website image which was cached by the browser. Yellow blocks indicate a hosted image which was not cached by the browser.

Figure 1. A wireframe representation of cached content by the Mozilla Firefox (1) and Google Chrome (2) web browsers on landing upon the www.bbc.co.uk/news page (taken on 01.05.17 at 13:31).

Figure 1 offers an indication of the volume of image content cached upon landing on a website, without interacting with it. As can be seen, imagery beyond the view of the user is cached, where in the case of Firefox, a user would need to scroll to the bottom of the site in order to visually witness all images which were cached on landing.

Figure 2 denotes the impact on the browser cache after a user scrolls down to view additional content on the page. The red lines indicate the new position of the screen, where approximately 30% of the website has been scrolled (45cm). Green blocks indicate any additionally

cached images following the scroll. As can be seen, even after scrolling, additional images remain cached beyond the sight of the user with the overall volume of images being cached increasing.

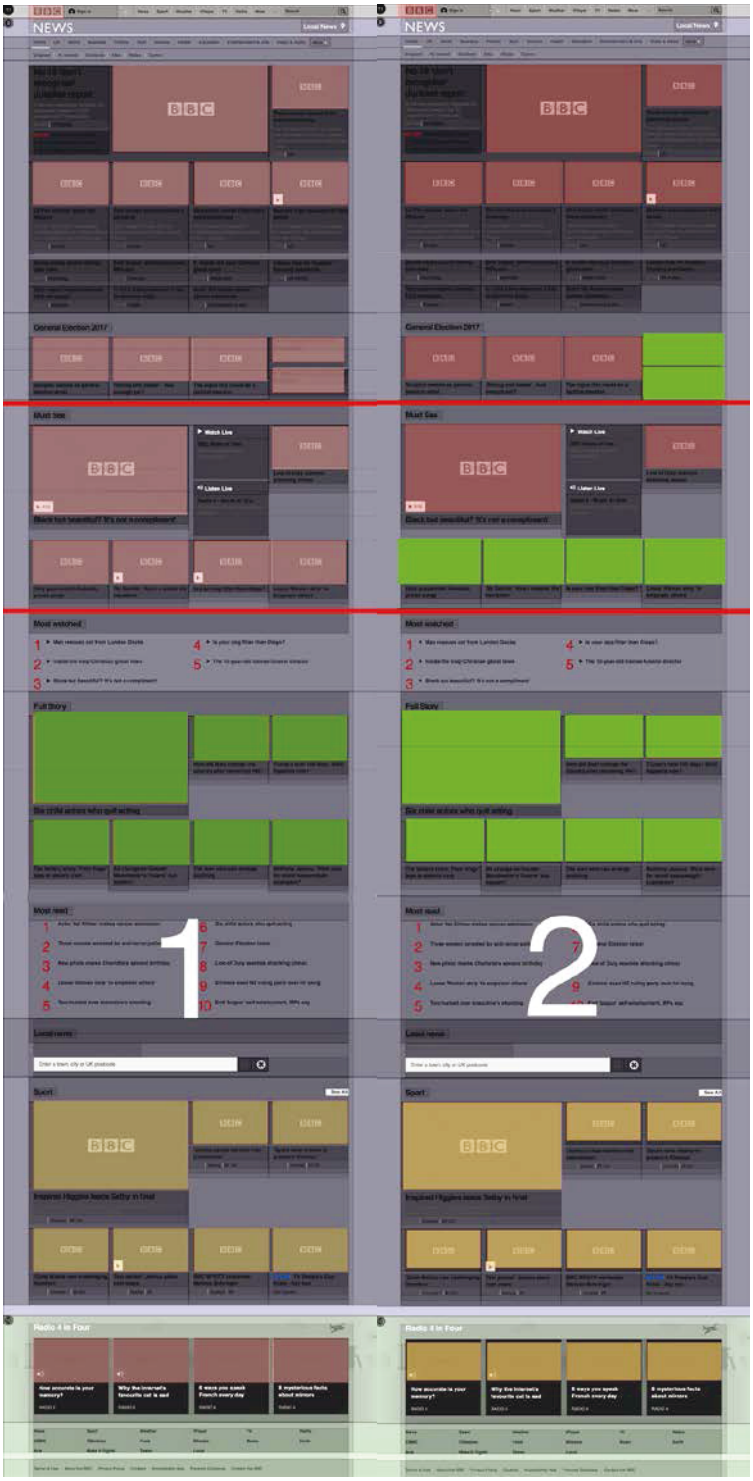

Figure 2. Following on from initial testing in Figure one, the browser (Firefox '1', Chrome '2') page has been scrolled down 45cm, simulating a user who has visited a page and proceeded to view the content. The screen position viewable to the user is identified between the two red lines. Green blocks indicate the additional images cached due to scrolling down the webpage.

Figures 1 and 2 suggest that the cache for each bowser reacts dynamically to the movement of the webpage itself and does not cache the entirety of the page on landing. This dynamic caching process ensures efficiency, preventing a user's browser cache from saving redundant website artefacts and overloading the local disk drive storage. However, from an evidential standpoint (bar the four images cached by Firefox at the bottom of the page), it is possible to identify an initial correlation between images cached and the user's view of the webpage on-screen, where the more of the page viewed, the more imagery is cached. Yet the caching of unseen imagery still provides an investigatory issue and it cannot be confirmed that all cached imagery would have been seen by a user. The examination of the cache following visits to www.bbc.co.uk/news highlights the challenges it poses in relation to the four cached image at the bottom of the website. These images are cached regardless of behaviour on landing when using the Mozilla Firefox browser but not cached on landing with Chrome. This appears to suggest that different browser caching algorithms may result in different volumes of cached content for the same website visit. Only following a complete scroll (100%) to the bottom of the web page, were all images present on the website were cached by both browsers.

To provide an overview, Table 1 provides a breakdown of Figures 1 and 2.

Table 1: A breakdown of cache statistics for the visit to *www.bbc.co.uk/news*

3.2 Testing & Results

Following the example provided in section 3.1, this section builds upon this work providing an analysis of the volume of image content cached from 10 test website visits in two scenarios, on-landing and after a 30% scroll. The results of caching by Google Chrome (version 58.0) and Mozilla Firefox (version 53.0) with a screen resolution of 1440*900, from 10 selected test websites, ranging in size and structure (to provide test diversity), are offered in Table 2. Testing was carried out in May 2017, with results consistent with website structures at this point in time. Testing took place on the Windows 10 platform.

Before testing, each browser's cache was cleared using the browser's in-built cleaning functionality. This was verified manually by locating and viewing the content of both browser's cache folder to confirm no content was present and via Nirsoft's ChromeCacheView (http://www.nirsoft.net/utils/chrome_cache_view.html) and MozillaCacheView(http://www.nirsoft.net/utils/mozilla_cache_viewer.html) forensic cache viewing applications (the focus of testing remained solely on live content). This ensured that no live cache content existed before each test website visit, preventing test contamination. For each visit, the web address for the site was inserted directly into the address bar and initiated following immediate loading of the web browser. To minimise impact on the cache, both browsers had their homepage set to 'www.google.co.uk' to prevent large volumes of images being cached from additional sources other than each test site, with any Google logo imagery being discounted from final test quantification of imagery. Once the page had indicated a complete load, cached image content was forensically extracted from each browser's resident cache folder (Chrome:- C:\Users\@@\AppData\Local\Google\Chrome\User Data\Default\Cache and Firefox:- C:\Users\@@\AppData\Local\Mozilla\Firefox\Profiles\@@\cache) using Nirsoft's appropriate tool (Chrome/Mozilla viewer) to a wiped removable device for visual interpretation and manual quantification. After each collection process, results were recorded and the cache was cleared and verified using the above process to prevent cache-contamination between tests, and the whole process repeated.

To provide a comprehensive overview of cache behaviour, Table 2 offers a breakdown of cache behaviour based on 10 randomly selected test websites.

Table 2: Cache behaviour documented from 10 website visits.

3.3 Cache behaviour analysed

The breakdown of results in Table 2 document the behaviour of the cache on both landing and via a 30% website scroll, designed to simulate a user who does not simply visit and leave a site, but take time to analyse content hosted upon it. Of the 10 websites analysed, both the size of the websites and the amount of imagery hosted on them vary in order provide diverse test data and simulate the impact of interactions with websites of different structure and length. Further, these sites are legitimate sites, not illegal sites (which would not be possible to test due to legal restrictions); yet still provide an insight into how the cache reacts to various web-site sizes and structures. Focus is maintained on quantifying cached imagery to simulate an IIoC investigation where imagery and thumbnails from hosted video content may be cached.

Although testing has focused on single website visits, a multiple website visit scenario has been considered. It should be noted that when a site was re-visited (an initial visit of a website, followed by a closure of the browser tab, reopen then revisit the webpage), typically two scenarios may occur. Where no changes to the website hosted imagery have occurred between the first visit and re-visit, typically no additional images are cached (for example, 30 images cached on first visit, 0 on the re-visit). Where a site has updated its content between visits, this additional imagery may be cached if it is in a location on the site which sits within a cacheable area.

3.3.1 Results on Landing

Of the 10 sites tested, only 3 (sites 1,2 & 4) cached all resident media on landing. As a result, sites 1 and 4 maintained the highest percentage of images cached which were not viewable by the user upon landing on the site. Of the remaining sites, volumes of cached imagery varied greatly, ranging from between 8 - 83%. Rates of caching could not be correlated to site size, and as a result, there is no consistent approach which can be adopted to determining how much of a site has been viewed by a defendant on landing. Although dependant on site design, in eight tests (excluding 3 & 5), website images were cached but not seen on landing.

3.3.2 On-scroll

For testing, a 30% scroll was implemented, simulating a user who lands on a website then proceeds to examine approximately a third of the content. In all cases (bar 1,2 & 4 which cached all images on landing) an increase in the number of images cached was witnessed. In addition, only cases 3, 5 (only Chrome) and 8 (only Firefox) resulted in all cached images being visible on-screen to a user after a 30% scroll. In all other cases, website images had been cached, but were not viewable to the user on-screen. The on-scroll testing however appears to suggest a correlation between the amount of the web page scrolled through (and therefore viewable) and the number of images cached regarding the chosen test sites and

web browsers. Although limitations regarding the size of testing carried out must be acknowledged, such inferences regarding scrolling vs. volume of images cached may be applicable in wider usage.

3.4 The impact of screen resolution

The results of table 2 suggest a link between viewable screen content and cached content. As a result, consideration of a user's screen resolution should be taken into account when attempting to establish cached content. Figure 3 provides an example comparison of cached content where a screen resolution of 1366*768 (1) vs. 1024*768 (2) is used. To provide an example test the Chrome browser is used. Not only does resolution have an impact on the volume of content seen on landing, but two additional images (18 vs. 16 images) are cached when a the larger screen resolution is utilised. As a result, screen resolution settings should also be taken into account when quantifying cached content during an investigation and considering what may have been physically seen by a user.

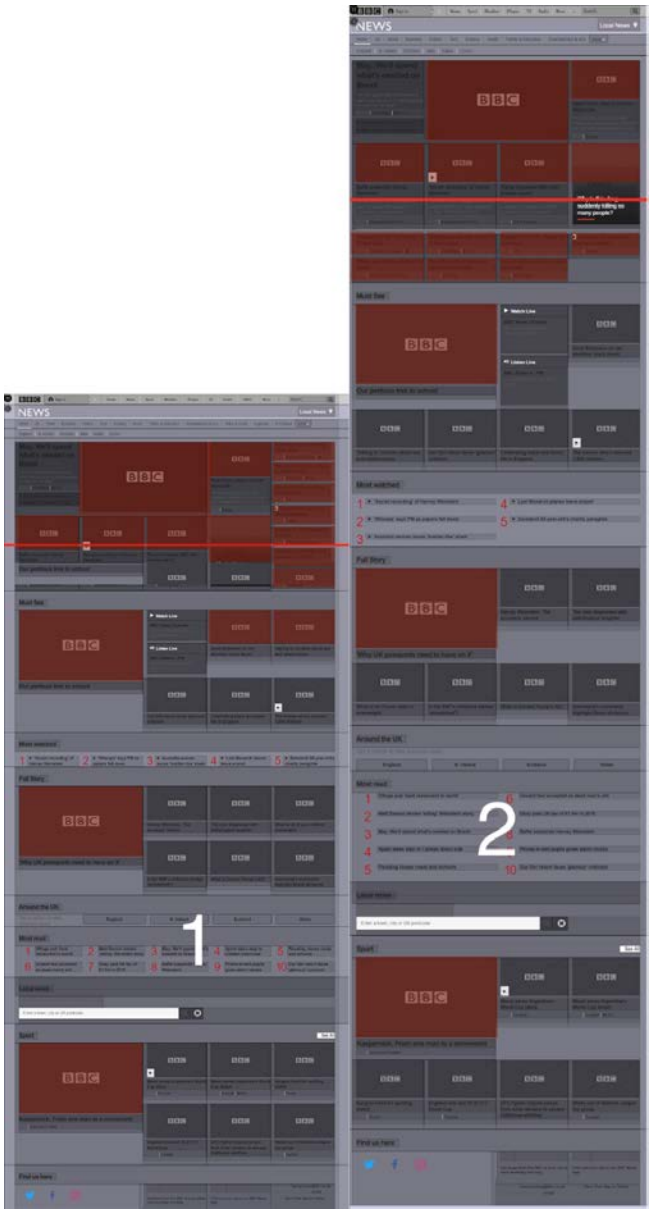

Figure 3: Wireframe 1 shows cached imaged using a screen resolution of 1366*768. Wireframe 2 shows cached imaged using a screen resolution of 1024* 768.

4 The Impact of testing on IIoC investigations

Following the testing documented in Table 2, it is clear that the cache presents an investigatory challenge in relation to IIoC and the presence of an image in the cache does not mean this has been physically viewed. This issue is noted by Herczeg (2014, p76-77).

> "Prosecuting someone for simply viewing websites containing child pornography images could lead to absurd and unfair results. It could mean that someone who accidentally or out of curiosity clicks on a link that takes him to child pornography material could be prosecuted for the act of viewing it. In order to avoid this risk, law enforcement should take into account evidence showing that the viewing of such material was accidental or otherwise unintentional. The prosecutor would look for example at the amount of the images stored into the cache file in order to determine if the Internet user was actively looking for child pornography or merely "stumbled" on the website" (Herczeg, 2014, p.76-77).

Fitzpatrick (2012, p915) states that "prosecutors often turn to the presence of temporary Internet files on the defendant's computer to show that by viewing the images; the defendant came to possess them because the computer generated the temporary Internet files". In *United States* v. Kain, 589 F.3d 945 (8th Cir. 2009), forensic expert 'Detective Mize (at 948) described 'temporary internet' files as locations where the computer temporarily stores web pages that were previously viewed' where the Court of Appeal held that 'the presence of child pornography in temporary internet and orphan files on a computer's hard drive is evidence of prior possession of that pornography' (at 950). This was interpreted by McBath (2012, p393) to mean the following;

> "Thus, the court held the evidence that the defendant possessed the images while the images resided on his computer screen to be sufficient, and copies of these images ultimately located in the cache were simply probative of that earlier viewing...In other words, the defendant's crime was complete at the moment he viewed the images on his monitor" (McBath, 2012, p393).

Yet the issue with these commentaries lies with the blanket assumption that cached content is proof of viewed content, where this interpretation of the cache cannot always be relied upon. Such sentiment is echoed by Gant (2012) who indicates that cached content is not on its own, evidence of viewed content, yet regularly this is assumed to be the case. Establishing whether a user has physically seen an IIoC on a website poses an investigatory issue and one which must be addressed by a forensic practitioner. This is an issue where a user visits a website but hosted imagery is not viewable on landing, meaning that in absence of any scrolling, they may move on to another site and never realise they had visited a site containing IIoC and that they had been cached. This issue also potentially exists with regards to determining the severity of an offence, where more severely categorised IIoC may exists on parts of a website which had not been viewed by a suspect upon landing, but had been subsequently cached.

Table 2 documents the relationship between scrolling and caching. All content which was viewable on-screen at any one time was cached in all test cases. However, the issue remains

that a percentage of unseen website imagery is also cached. This content is unquantifiable in the sense that it differs from website to website, and therefore it is not possible to establish definitively from a post mortem analysis of cached files alone to identify which files were viewed.

What is key to note is that every website may and likely will behave differently, therefore where a question of viewing IIoC is raised, control tests must be carried out on a site in question (subject to requisite legislation permitting recognisance on a known illegal site) to scrutinise the cache behaviour, replicating a defendant's browser setup and potential movements. Even in such cases, it may not be possible with the requisite accuracy needed to establish a factual account of the user's 'viewing' actions, particularly where a site has subsequently changed after a defendant has been arrested and devices seized. Testing within this work took place on legitimate mainstream websites, providing an indication as to how browser caches perform in these circumstances. Cache behaviour regarding indecent websites, which may employ less common structures are likely to impact cache behaviours. A limitation of this work is the inability to examine browser cache behaviour following indecent website visits, and only an inference can be made with regards to scrolling and the volume of images being cached. Further testing would be needed, and given the diversity of potential website structures available (where some IIoC websites may be archaic or akin to websites which stem from a single host configuration), each case would almost certainly be in need of testing specific to each website.

To summarise, Table 2 allows the following assumptions to be made.

1. When a website is visited for the first time, not all of the website's imagery content may be cached in all cases.
2. Imagery which has not been visible on-screen is cached, meaning it is not possible to reliably establish whether a user has seen imagery cached from a website visit, from an analysis of the cache alone. Testing must be undertaken on a suspect website in question, in order to try and replicate the suspect's cache and correlate this to associated actions.
3. When a user scrolls through more of a websites content, this will likely increase the volume of content cached from the website.

4.1 The impact on CJA88 Section 160(2)(b)

The inability to definitively identify which images have been viewed by a user on-screen may cast doubt on the applicability of the defence under CJA88 Section 160(2)(b) in relation to IIoC in the cache. A defence which suggests reliance on establishing 'sight' needs to be supported by reliable evidence of what content has been shown to a defendant on screen. Given that this is likely not possible, arguably the application of this defence should be treat with caution. Following legal literature, the presence of an assumption that cached files are viewed files may prevent a defendant from relying on the defence in this scenario. However it remains a viable possibility, where the host site responsible for the cached imagery must have its structure thoroughly investigated before any assumptions on sight can even be considered. Similarly, concerns are also raised about the use of a possession offence in relation to the cache, as it is feasible to know of the cache (making a defendant potentially liable for its content), but

never realise that it contains IIoC as they may have never been seen on-screen. This potentially raises issues of inconsistency of the application of possession related offences in cache contexts.

5 Conclusions

This article is one of the first studies to examine the functionality of the Google Chrome and Mozilla Firefox browser caches in an attempt to assess the possibility of identifying which browser cached images have been physically viewed by a user on-screen. Testing has highlighted inconsistent cache behaviour, meaning that it may not possible to make an accurate assumption of which images were viewed by a user based on cached content alone. Whilst this work has focused on mainstream website testing, it has allowed inferences regarding cached content volumes and links to website scrolling to be established, which may be applicable in cases involving sites hosting IIoC.

References

Altheide, C. and Carvey, H., (2011). Digital forensics with open source tools. Elsevier.

Atkins v DPP; Goodland v DPP [2000] 2 Cr. App. R. 248

Casey, E., (2009). Handbook of digital forensics and investigation. Academic Press.

CPS (2017) 'Indecent Images of Children (IIOC)' Available at: http://www.cps.gov.uk/legal/h_to_k/indecent_images_of_children/ (Accessed: 3rd May 2017)

Digital Detective (2017) 'NetAnalysis' Available at: http://www.digital-detective.net/digital-forensic-software/netanalysis/ (Accessed: 3rd May 2017)

Fitzpatrick, Julianne C. (2012) "People v. Flick: Modernizing Michigan's Child-Pornography Statute to Criminalize Viewing in Response to Evolving Internet Technology." New England Law Review 46(4), pp.909-930

Gant, Katie. (2012) "Crying over the Cache: Why Technology has Compromised the Uniform Application of Child Pornography Laws." Fordham Law Review 81(1), pp.319-364.

Habben, James (2015) 'FIREFOX CACHE2 STORAGE BREAKDOWN' Available at: https://www.guidancesoftware.com/blog/digital-forensics/2015/02/11/firefox-cache2-storage-breakdown (Accessed: 4th January 2018)

Herczeg, J., (2014). 'Actual Problems of Possession and Viewing Child Pornography in Internet'. Jura: A Pecsi Tudomanyegyetem Allam-es Jogtudomanyi Karanak tudomanyos lapja, p.70.

Horsman, G., (2016). Digital forensics: Understanding the development of criminal law in England and Wales on images depicting child sexual abuse. Computer Law & Security Review, 32(3), pp.419-432.

Howard, T.E., (2004). 'Don't cache out your case: Prosecuting child pornography possession laws based on images located in temporary Internet files'. Berkeley Technology Law Journal, pp.1227-1273.

httparchive (2017) 'Interesting stats' Available at: httparchive.org/interesting.php (Accessed: 3rd October 2017)

Magnet Forensics (2017) 'IEF Feature Focus – Rebuilding Webpages' Available at: https://www.magnetforensics.com/computer-forensics/ief-feature-focus-rebuilding-webpages/ (Accessed: 3rd May 2017)

Marin, G. (2008) "Possession of Child Pornography: Should You Be Convicted When the Computer Cache Does the Saving for You." *Fla. L. Rev.* 60(5), p.1205-1236.

McBath, J. E. (2012) "Trashing our System of Justice - Overturning Jury Verdicts where Evidence is Found in the Computer's Cache." *Am. J. Crim. L*. 39(3), p.381-424.

Miller, B.D., 2016. Above the Fold: Understanding the Principles of Successful Web Site Design. Simon and Schuster.

Ritchie, John (2012) 'Firefox Cache Format and Extraction' Available at: https://articles.forensicfocus.com/2012/03/09/firefox-cache-format-and-extraction/ (Accessed: 4th January 2018)

Soasta (2015) 'Page bloat update: The average web page is more than 2 MB in size' Available at: https://www.soasta.com/blog/page-bloat-average-web-page-2-mb/ (Accessed: 3rd May 2017)

The Chromium Projects (n.d.) '' Available at: https://www.chromium.org/developers/design-documents/network-stack/disk-cache (Accessed: 4th January 2018)

United States v. Kain, 589 F.3d 945 (8th Cir. 2009)

United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002)

United States v. Goff, 501 F.3d 250, 258 (3d Cir. 2007)

Wall, D. ed., 2017. Crime and deviance in cyberspace. Routledge.